ARMY RESEARCH LABORATORY

Human Subject Research Protocol: Computer-Aided Human Centric Cyber Situation Awareness: Understanding Cognitive Processes of Cyber Analysts

by Peng Liu, Robert Erbacher, William Glodek, Renee E. Etoty, and John Yen

ARL-TR-6731 November 2013

NOTICES

Disclaimers

The findings in this report are not to be construed as an official Department of the Army position unless so designated by other authorized documents.

Citation of manufacturer’s or trade names does not constitute an official endorsement or approval of the use thereof.

Destroy this report when it is no longer needed. Do not return it to the originator.

Army Research Laboratory
Adelphi, MD 20783-1197

ARL-TR-6731 **November 2013**

Human Subject Research Protocol: Computer-Aided Human Centric Cyber Situation Awareness: Understanding Cognitive Processes of Cyber Analysts

Peng Liu and John Yen
College of Information Sciences and Technology
The Pennsylvania State University
301F IST Building, University Park, PA 16802

Robert Erbacher, William Glodek, and Renee E. Etoty
Computational and Information Sciences Directorate, ARL

REPORT DOCUMENTATION PAGE	*Form Approved* *OMB No. 0704-0188*

1. REPORT DATE *(DD-MM-YYYY)* November 2013	**2. REPORT TYPE** Final	**3. DATES COVERED (From - To)** October 2012 to September 2013

4. TITLE AND SUBTITLE Human Subject Research Protocol: Computer-Aided Human Centric Cyber Situation Awareness: Understanding Cognitive Processes of Cyber Analysts	**5a. CONTRACT NUMBER** **5b. GRANT NUMBER** **5c. PROGRAM ELEMENT NUMBER**
6. AUTHOR(S) Peng Liu, Robert Erbacher, William Glodek, Renee E. Etoty, and John Yen	**5d. PROJECT NUMBER** **5e. TASK NUMBER** **5f. WORK UNIT NUMBER**
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) U.S. Army Research Laboratory ATTN: RDRL-CIN-D 2800 Powder Mill Road Adelphi, MD 20783-1197	**8. PERFORMING ORGANIZATION REPORT NUMBER** ARL-TR-6731
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) U.S. Army Research Office (ARO)	**10. SPONSOR/MONITOR'S ACRONYM(S)** **11. SPONSOR/MONITOR'S REPORT NUMBER(S)**

12. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release; distribution unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The purpose of this research study is to understand the cognitive process of cyber-security analysts when defending cyber-attacks. Twelve subjects have been recruited from Adelphi Laboratory Center (ALC) of the U.S. Army Research Laboratory (ARL). Each participant is asked to do one or more sessions so that the outcomes can be compared to answer research questions. In the study, subjects play the role of cyber security analysts and are asked to analyze data sources (e.g., network topology and policy, IDS alerts, firewall logs) of the computer network of a large organization to identify suspected attacks, type of attacks, key events or evidence, and associated hypotheses or questions to guide further investigation toward drawing a conclusion. The subjects receive training for the task, complete Pre-Task and Post-Task Questionnaires, and receive no compensation for participating in the study. This research protocol is for continuing the study in collaboration with co-PI's and Associate Investigator of ARL.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON** (301) 394-1835
a. REPORT Unclassified	**b. ABSTRACT** Unclassified	**c. THIS PAGE** Unclassified	UU	26	**19b. TELEPHONE NUMBER** (*Include area code*) Renee E. Etoty

Contents

List of Figures

1. Research Background

Cyber analysts play a critical role in cyber defense. Their tasks are difficult due to the overwhelming amount of network traffic, noise-abundant data (e.g., false positive alerts), and increasing complexity and sophistication of the cyber attacks. While experienced cyber analysts are able to perform this complex task effectively, our understanding about the cognitive process of network analysts is rather limited. These difficulties present challenges to maintaining effective cyber defenses from the psychosocial perspective, which includes cognitive processes of cyber analysts. An example of cyber defense operation in the Army is Computer Network Defense Service Provider (CNDSP), operated in ARL's Computational and Information Sciences Directorate (CISD), which provides cyber defense for a broad network relevant to the Army.

The challenges of cyber defense place high demand on each analyst's capability for data processing and analytical reasoning. Hence, an efficient analytical reasoning support system is urgently needed to assist analysts in evidence exploration, information correlation, hypothesis maintenance, and reasoning. Even though it is desirable to leverage the experience of expert cyber analysts to support junior analysts, the experience of expert analysts remains untapped, due to the difficulty of eliciting, capturing, sharing, and transferring experiential knowledge, which has been referred to as the "knowledge acquisition bottleneck" in the literature of artificial intelligence (*1*).

Logic-based models are widely used to represent experts' knowledge and preferences. One crucial problem in cyber analysis is alert correlation given that IDS alerts are redundant and noisy. Most cyber analysis tools use rules and logical patterns to help analysts verify or invalidate alerts (*2*, *3*). Logical attack graphs can also be generated by logic reasoning based on specified rules (*4*). Given a network with known vulnerabilities, a logical attack graph can be easily generated, presenting all possible cyber-attack paths (*4*). By using rules to represent experience-based knowledge, Chen et al. (*5*) point out that relaxing the conditions of the rules is critical to utilize experience efficiently. However, pattern-based representations are inherently inflexible and many patterns may require exceptions. They also require knowledge to be highly formalized and structured. These limitations reduce the effectiveness of such tools and approaches to adapt to new attack strategies.

Research in cognitive science has shown that humans have limited working memory and information processing capabilities (*6*). Typically, the large amount of data generated by existing cyber-attack detection tools far exceeds the analysts' cognitive capabilities. Grounded in perceptual and cognitive theory, many visual analytical tools have been developed to facilitate sense-making. Sense-making is the theoretical foundation to achieve understanding from the use of analytical reasoning. It involves information seeking, observation analysis, insight development and result production (*7*). Although it is known that experience plays an important role in sense-making, there is not a clear definition of experience in the literature.

In the context of cyber analysis, experience facilitates an analyst's sense-making by providing guidance through its four processes illustrated in figure 1: information seeking, observation analysis, insight development, and result/conclusion production. These four processes are connected by three guiding questions: (1) Which data source should be examined? (2) What is implied by the evidence? (3) How to verify the hypothesis? Unfortunately, most current logic-based representation methods are often unable to capture the analytical reasoning process of analyst at this level of detail.

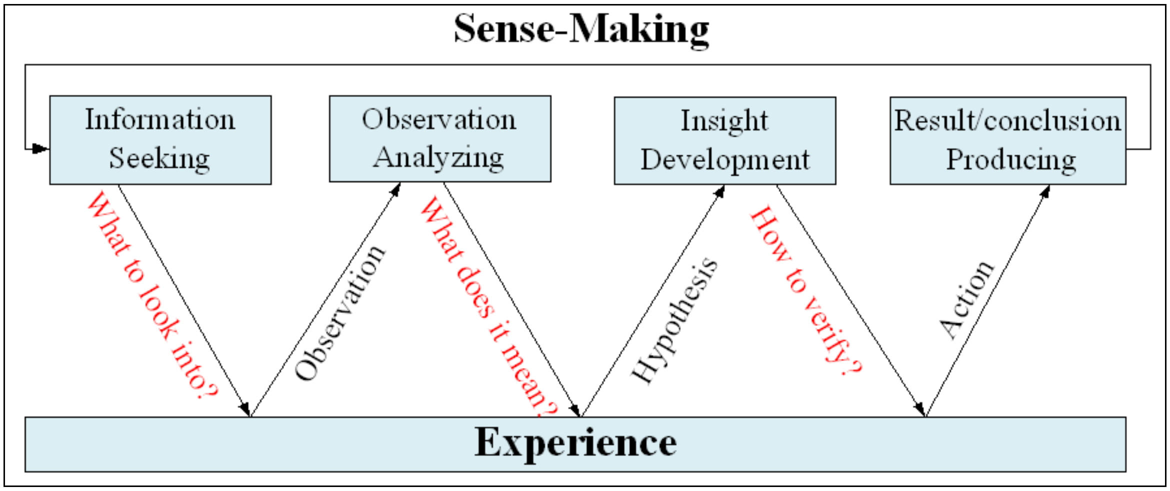


Figure 1. The Role of Experience in Analytical Reasoning Process.

1.1 Cognitive Processes of Network Security Analysts

The experience of cyber analysis can be characterized by a space consisting of three dimensions: (1) human analyst, (2) analysis task, and (3) time. This world is used to represent experience and knowledge. A point in this three-dimension world is the triple: $P=(a_m, t_n, T_t)$, which refers to the sense-making actions performed by analyst a_m in performing task t_n at time T_t. The upper right corner of figure 2 describes the reasoning process of analyst *a* while performing task *t* from time *T1* to *T2*.

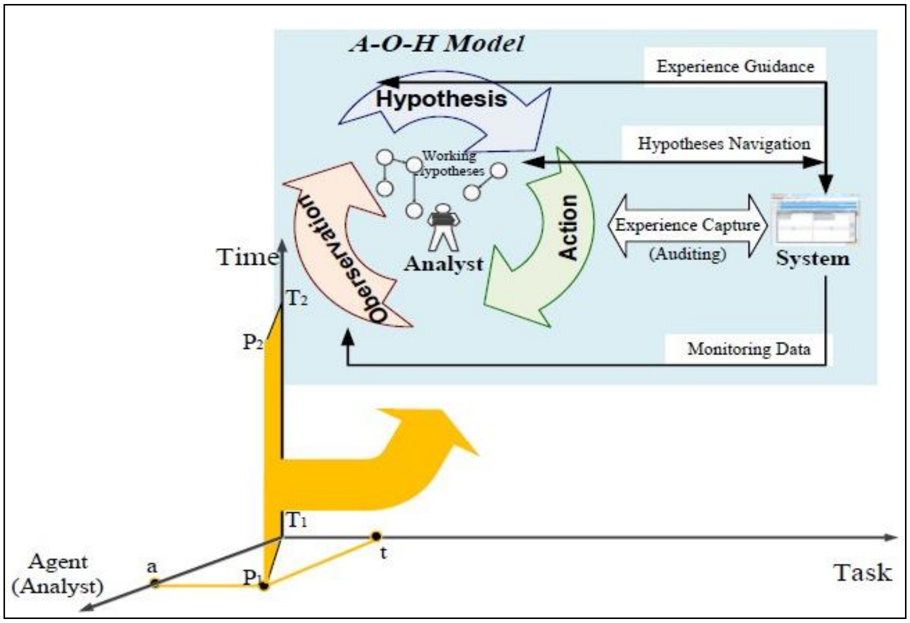


Figure 2. An analyst works with the experience-aided reasoning support system.

1.1.1 The "A-O-H" Model of Cyber Security Analysts' Cognitive Processes

Inspired by the sense-making theory discussed earlier, we model the analytical reasoning process of cyber analysts using three key cognitive constructs: "Action," "Observation," and "Hypothesis" (i.e., the "A-O-H" model in figure 2). *Actions* refer to the analysts' evidence exploration activities; *observations* refer to the observed data/alerts considered relevant by the analyst; and *hypotheses* represent the analysts' awareness and assumptions in certain situations. These three constructs iterate and form reasoning cycles: the initial trigger could be a suspicious observation (e.g., an IDS alert or denied accesses in firewall logs). This observation may result in new or updated hypotheses (all the hypotheses maintained by an analyst are called "working hypotheses"); each hypothesis could trigger further actions to confirm or disconfirm it. New actions will lead to new observations; thereby, another "A-O-H" cycle begins. The loop ends when a conclusion is drawn or when all relevant observations from the available data have been analyzed.

1.1.2 Computational Representation of Cyber Security Analysts' Cognitive Processes

From the perspective of computational representation of analysts' cognitive processes, "actions" and "observations" in the "A-O-H" model have a structured representation because they are explicit facts. However, capturing analysts' mental reasoning can be quite complicated if we choose a formal representation. Therefore, we chose a "hypothesis" representation that is easiest for the analyst to describe: free text. We combine each action with its resulting observation(s) into a pair, called an "Experience Unit (EU)", to denote the external activities and related contexts. We associate each hypothesis to the corresponding EU. Sometimes, the observations in an EU can lead to multiple alternative hypotheses. Therefore, an EU, in general, can be associated with multiple hypotheses. An "E-Tree" is constructed to represent the reasoning process by connecting the external analytical actions and observations ("EUs") with the internal analytical reasoning ("hypotheses"). The branches connecting an EU with a set of hypotheses illustrate that these disjunctive hypotheses are created in the light of this EU's observation. In order to facilitate the analyst in browsing the hypotheses and navigating among them, we further extract the hypotheses from the E-tree to form a hypothesis tree (i.e., "H-Tree"). An example of E-tree and corresponding H-tree is shown in figure 3. The exemplar E-tree shows the first experience unit (EU 1) leads to two alternative hypotheses (Hypothesis 1 and Hypothesis 2). Each hypothesis node in the E-tree and the H-tree is associated with a "truth value", which can be "unknown," "true," or "false". These truth values are indicated by the color of hypothesis nodes in figure 3: those with red color indicate "false" (i.e., rejected hypothesis), and those with green color indicate "true" (i.e., confirmed hypothesis).

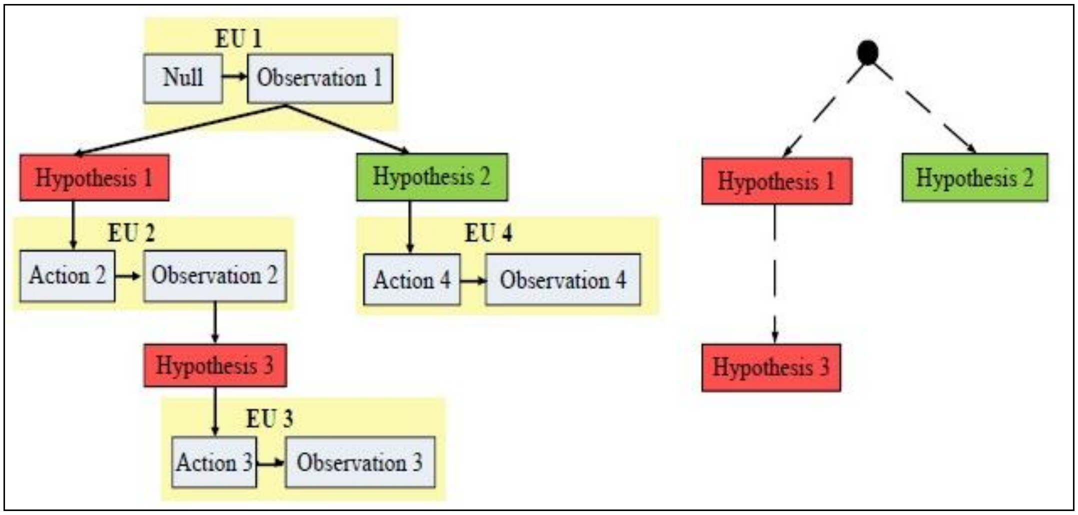


Figure 3. An Example of E-Tree and its H-Tree.

1.1.3 A Tool for Capturing the Cognitive Processes of Network Security Analysts

Based on the A-O-H model, an analytical reasoning process capture and support tool, Analytical Reasoning Support for Cyber Analysis (ARSCA), has been developed to enable the analytical reasoning process of cyber analysts to be captured in a non-intrusive way. The tool supports and captures the *actions* of analysts in filtering data by one or more conditions (e.g., filter Firewall logs for a particular destination port or filter on an alert to exclude an IP address), and in selecting data entries (e.g., selecting one or more entries in the Firewall log). The tool also captures analysts' *observations* through his/her selection of one or more data entries (often after filtering the raw data) or taking a screen shot by selecting areas of interests (e.g., part of a network topology or a visualization display). A key function of the tool is to enable the analyst to write down his/her thoughts or *hypotheses* based on the current set of observations. As the analyst gathers additional observations (some of which may be inspired by the current hypotheses), additional hypotheses can be created, and will be organized under the current hypothesis. More than one competing hypotheses can be generated by the analyst using the "create sibling hypothesis" feature in the tool. ARSCA provides two major functions using two views: (1) a data monitoring view for the analyst to choose data sources, filter entries from a source, and select entries of interest, and (2) an analysis view for the analyst to easily view and navigate the E-tree and H-tree for tracking and investigating multiple hypotheses. The analyst can easily switch between the two views. The analysis view also enables the analyst to easily switch his/her "focus of attention" among multiple hypotheses in the H-tree. The tool also provides reasoning support to maintain the consistency of the truth values of the hypotheses.

The VAST Challenge is a visual analytics contest organized yearly. Based on cyber analysis data of VAST Challenge, multiple scenarios of network analysis task have been developed using ARSCA.

2. Research Objective

The long-term objective of this research is to improve our understanding of the cognitive process of network analysts, especially those related to their analytical reasoning, so that training and analytical reasoning support tools (including visualization) for network analysts can be improved based on the improved understanding. More specifically, this research aims to conduct an initial validation of the A-O-H model using a tool for non-intrusive capture and support of the analytical reasoning process of network analysts (i.e., ARSCA).

3. Instrumentation and Facilities

Equipment

- All equipments used in the experiment are not connected to the internet.
- One laptop (without internet connection), manufactured by a commercial PC vendor (e.g., Lenovo or Dell) for sale to the public, running Windows operating system. The laptop is provided by the research team of Penn State University. One or more ARL-owned laptops, manufactured by a commercial PC vendor (e.g., Dell), may also be provided.
- Software for the analytical reasoning support tool is installed on the laptops.
- The laptops are also loaded with a pre-task questionnaire, training video and instruction, a post-task questionnaire, a user manual of the tool, and detailed step-by-step instructions for the procedure. The materials are organized according to the four major steps of the procedure using four folders: (1) Step 1: Pre-task Questionnaire, (2) Step 2: Training, (3) Step 3: Doing the task, and (4) Step 4: Post-task Questionnaire.

- One projector connected to the laptop. The projector is purchased by Penn State University. One or more ARL-owned projectors may also be provided.
- A keyboard connected to the laptop
- A mouse connected to the laptop

Safety Releases for Equipment or Apparatus

No safety releases are required.

Facility

The study will be conducted in room 2F014 and adjacent rooms in Building 204 of Adelphi Laboratory Center, MD.

Standard Operating Procedures for Courses or Facilities

There is currently no SOP on file for the facility.

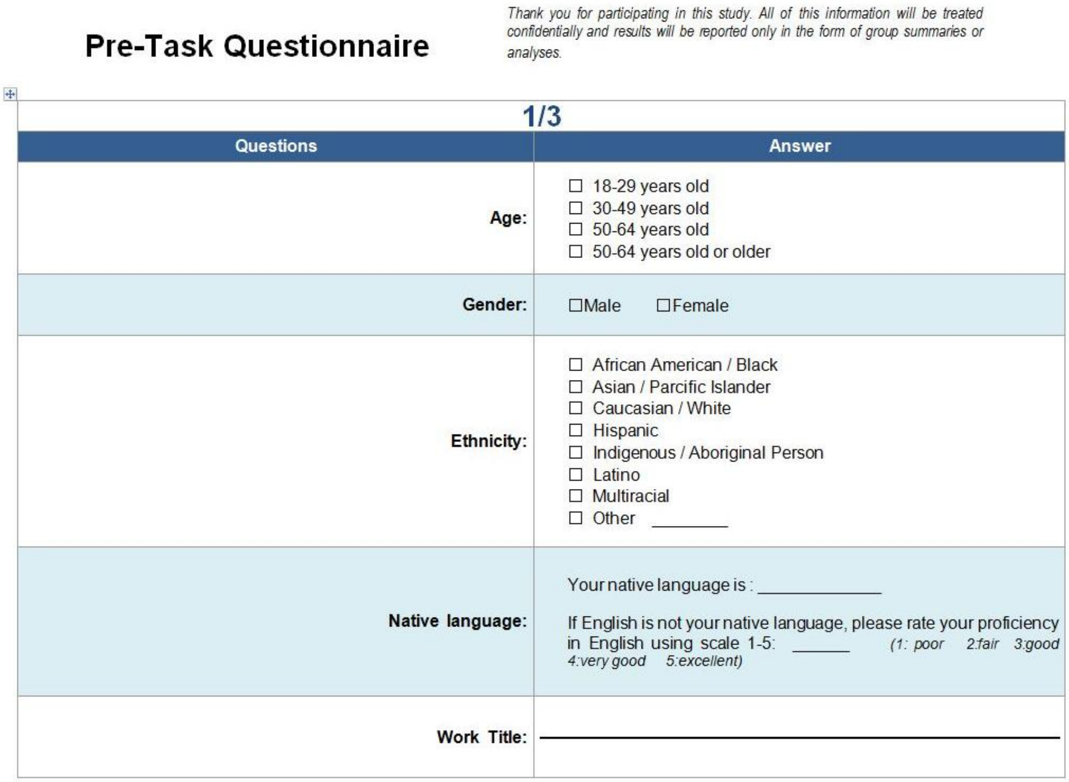
4. Materials, Tests, Tasks, and Stimuli

Questionnaires, Surveys, Psychometric Tests, or Forms

Two questionnaires are used in the study: (1) a pre-task questionnaire and (2) a post-task questionnaire.

Pre-Task Questionnaire

The Pre-task questionnaire includes three types of questions: (1) questions about demographic information of the subject (e.g., age, gender, ethnicity, and native language), (2) five-level Likert question items about knowledge and experience regarding cyber security, and (3) five-level Likert question items regarding analytical reasoning style of the subject. The complete Pre-Task Questionnaire is shown in figure 4.



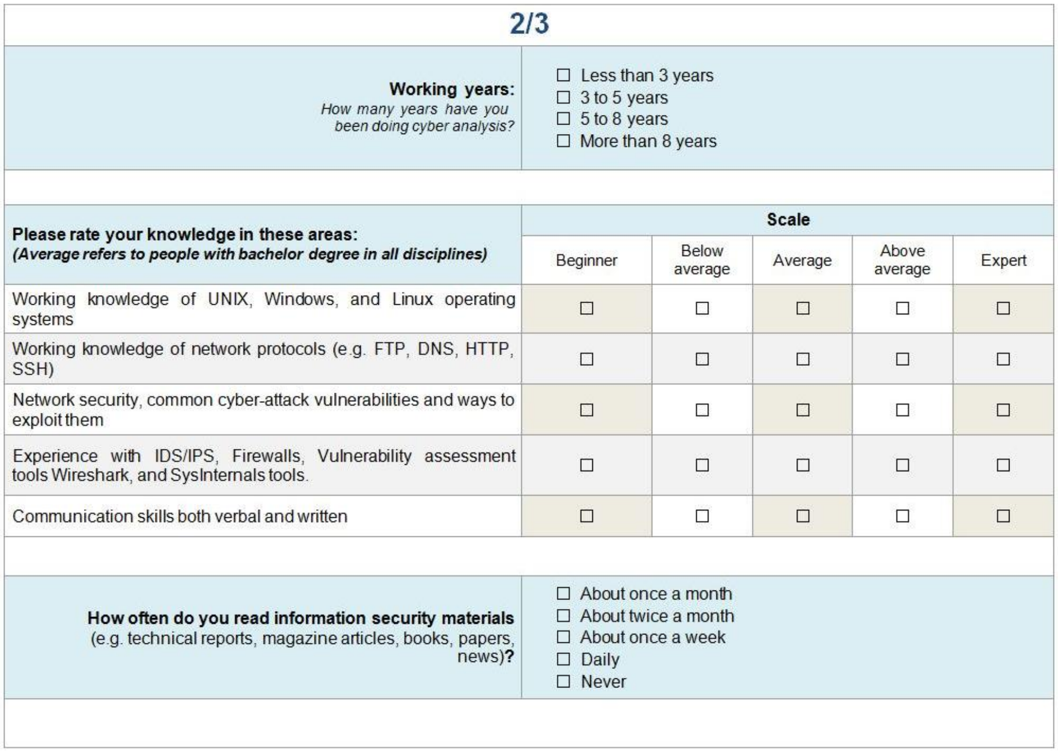
Pre-Task Questionnaire

Thank you for participating in this study. All of this information will be treated confidentially and results will be reported only in the form of group summaries or analyses.

1/3

Questions	**Answer**
Age:	□ 18-29 years old □ 30-49 years old □ 50-64 years old □ 50-64 years old or older
Gender:	□Male □Female
Ethnicity:	□ African American / Black □ Asian / Parcific Islander □ Caucasian / White □ Hispanic □ Indigenous / Aboriginal Person □ Latino □ Multiracial □ Other ________
Native language:	Your native language is : ______________ If English is not your native language, please rate your proficiency in English using scale 1-5: ______ *(1: poor 2:fair 3:good 4:very good 5:excellent)*
Work Title:	____

Figure 4. Page 1 of pre-task questionnaire.



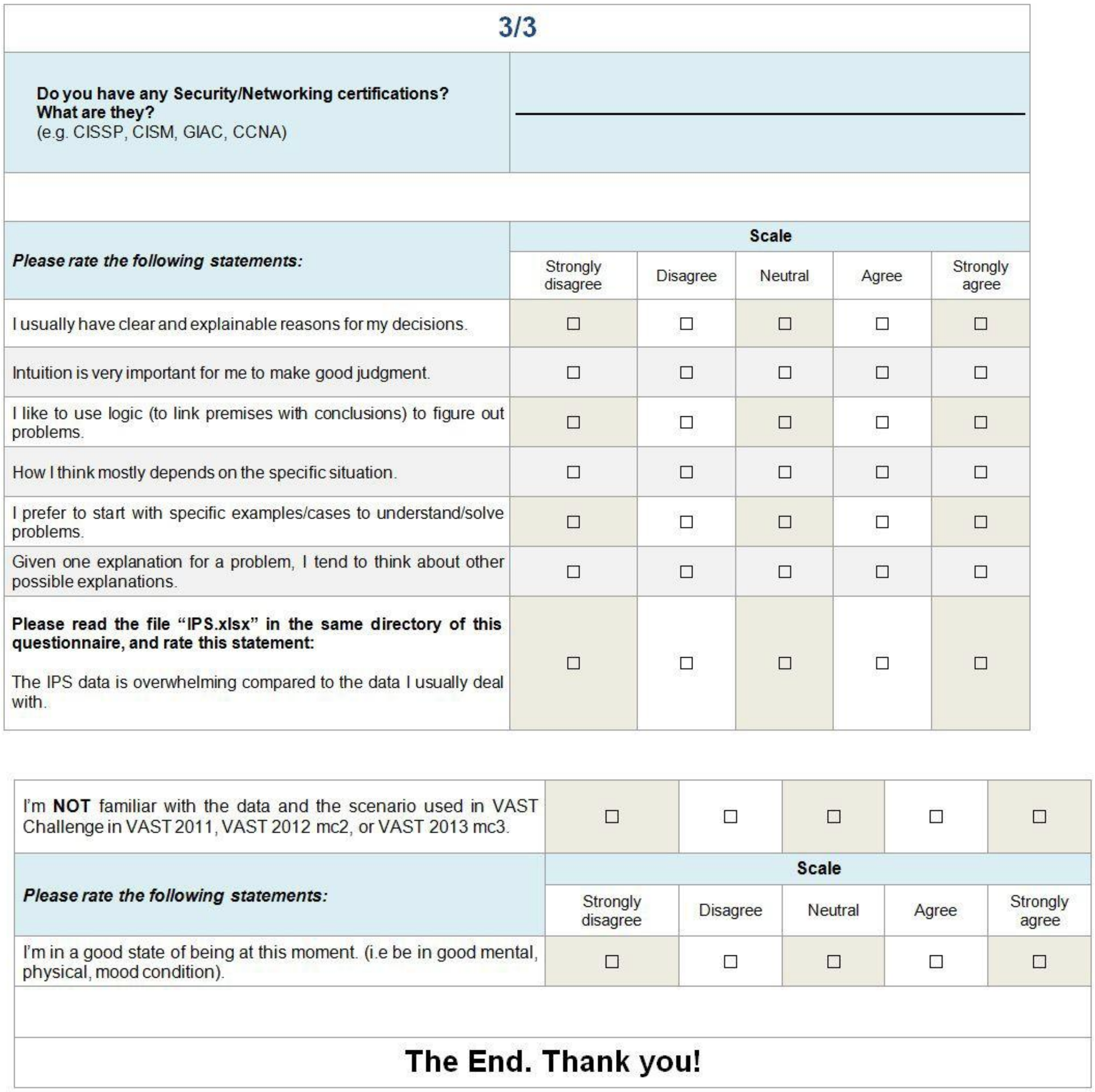
2/3

Working years: *How many years have you been doing cyber analysis?*	□ Less than 3 years □ 3 to 5 years □ 5 to 8 years □ More than 8 years

Please rate your knowledge in these areas: ***(Average refers to people with bachelor degree in all disciplines)***	**Scale**				
	Beginner	Below average	Average	Above average	Expert
Working knowledge of UNIX, Windows, and Linux operating systems	□	□	□	□	□
Working knowledge of network protocols (e.g. FTP, DNS, HTTP, SSH)	□	□	□	□	□
Network security, common cyber-attack vulnerabilities and ways to exploit them	□	□	□	□	□
Experience with IDS/IPS, Firewalls, Vulnerability assessment tools Wireshark, and SysInternals tools.	□	□	□	□	□
Communication skills both verbal and written	□	□	□	□	□

How often do you read information security materials (e.g. technical reports, magazine articles, books, papers, news)**?**	□ About once a month □ About twice a month □ About once a week □ Daily □ Never

Figure 5. Page 2 of pre-task questionnaire.



3/3

Do you have any Security/Networking certifications? What are they?
(e.g. CISSP, CISM, GIAC, CCNA) ______________________________

Please rate the following statements:	**Scale**				
	Strongly disagree	Disagree	Neutral	Agree	Strongly agree
I usually have clear and explainable reasons for my decisions.	□	□	□	□	□
Intuition is very important for me to make good judgment.	□	□	□	□	□
I like to use logic (to link premises with conclusions) to figure out problems.	□	□	□	□	□
How I think mostly depends on the specific situation.	□	□	□	□	□
I prefer to start with specific examples/cases to understand/solve problems.	□	□	□	□	□
Given one explanation for a problem, I tend to think about other possible explanations.	□	□	□	□	□
Please read the file "IPS.xlsx" in the same directory of this questionnaire, and rate this statement: The IPS data is overwhelming compared to the data I usually deal with.	□	□	□	□	□

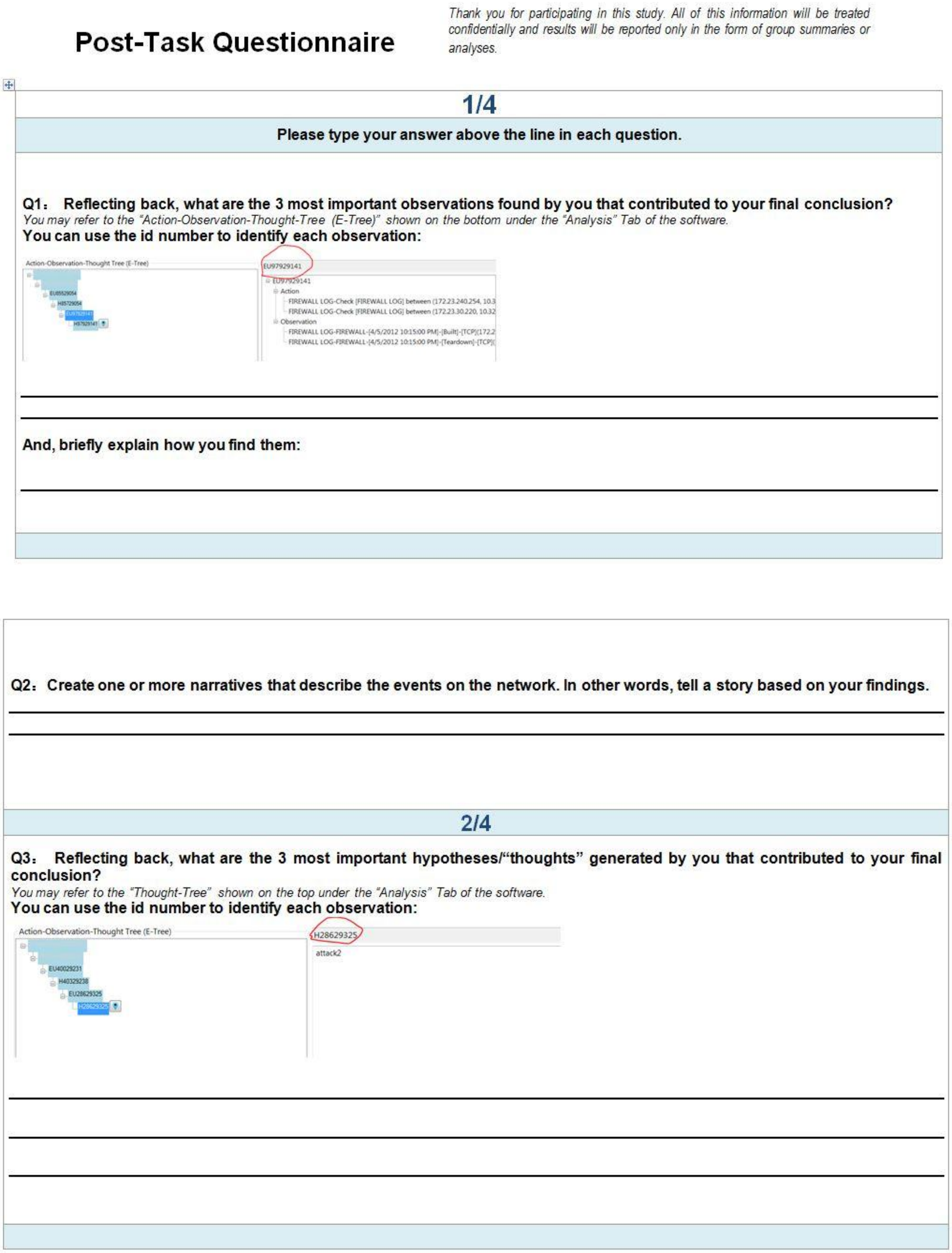
I'm **NOT** familiar with the data and the scenario used in VAST Challenge in VAST 2011, VAST 2012 mc2, or VAST 2013 mc3.	□	□	□	□	□
Please rate the following statements:	**Scale**				
	Strongly disagree	Disagree	Neutral	Agree	Strongly agree
I'm in a good state of being at this moment. (i.e be in good mental, physical, mood condition).	□	□	□	□	□

The End. Thank you!

Figure 6. Page 3 of pre-task questionnaire.

Post-Task Questionnaire

The post-task questionnaire includes (1) questions for the subject to reflect on concerning the task and to identify important observations important hypotheses, unanswered questions, how they are found, and the story (e.g., a cyber-attack) that connects them; (2) five-level Likert question items regarding the subject's self-assessment about his/her performance on the task, and (3) five-level Likert question items about whether the Action-Observations-Thought(Hypothesis) (A-O-H) model captures the subject's analytical reasoning process. The complete post-task questionnaire is provided in figure 7.



Post-Task Questionnaire

Thank you for participating in this study. All of this information will be treated confidentially and results will be reported only in the form of group summaries or analyses.

1/4

Please type your answer above the line in each question.

Q1： Reflecting back, what are the 3 most important observations found by you that contributed to your final conclusion?
You may refer to the "Action-Observation-Thought-Tree (E-Tree)" shown on the bottom under the "Analysis" Tab of the software.
You can use the id number to identify each observation:

EU97929141

```
EU97929141
  Action
    FIREWALL LOG-Check [FIREWALL LOG] between (172.23.240.254, 10.3
    FIREWALL LOG-Check [FIREWALL LOG] between (172.23.30.220, 10.32
  Observation
    FIREWALL LOG-FIREWALL-[4/5/2012 10:15:00 PM]-[Built]-[TCP](172.2
    FIREWALL LOG-FIREWALL-[4/5/2012 10:15:00 PM]-[Teardown]-[TCP](
```

______

______

And, briefly explain how you find them:

______

Q2：Create one or more narratives that describe the events on the network. In other words, tell a story based on your findings.

______

______

2/4

Q3： Reflecting back, what are the 3 most important hypotheses/"thoughts" generated by you that contributed to your final conclusion?
You may refer to the "Thought-Tree" shown on the top under the "Analysis" Tab of the software.
You can use the id number to identify each observation:

H28629325

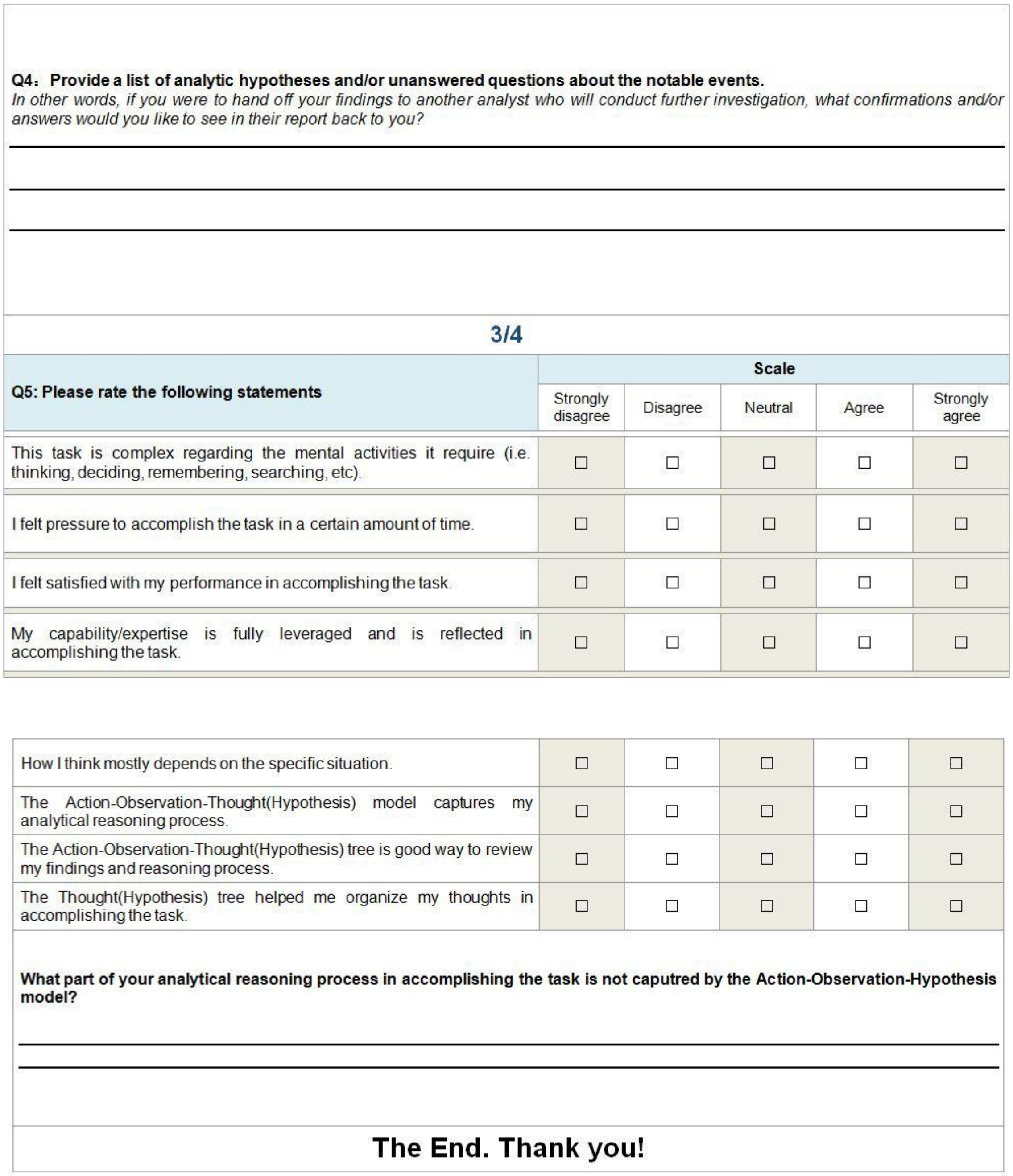
attack2

______

______

______

Figure 7. Pages 1-2 of the post-task questionnaire.



Q4：Provide a list of analytic hypotheses and/or unanswered questions about the notable events.
In other words, if you were to hand off your findings to another analyst who will conduct further investigation, what confirmations and/or answers would you like to see in their report back to you?

____

____

____

3/4

Q5: Please rate the following statements	**Scale**				
	Strongly disagree	Disagree	Neutral	Agree	Strongly agree
This task is complex regarding the mental activities it require (i.e. thinking, deciding, remembering, searching, etc).	□	□	□	□	□
I felt pressure to accomplish the task in a certain amount of time.	□	□	□	□	□
I felt satisfied with my performance in accomplishing the task.	□	□	□	□	□
My capability/expertise is fully leveraged and is reflected in accomplishing the task.	□	□	□	□	□
How I think mostly depends on the specific situation.	□	□	□	□	□
The Action-Observation-Thought(Hypothesis) model captures my analytical reasoning process.	□	□	□	□	□
The Action-Observation-Thought(Hypothesis) tree is good way to review my findings and reasoning process.	□	□	□	□	□
The Thought(Hypothesis) tree helped me organize my thoughts in accomplishing the task.	□	□	□	□	□

What part of your analytical reasoning process in accomplishing the task is not caputred by the Action-Observation-Hypothesis model?

____

____

The End. Thank you!

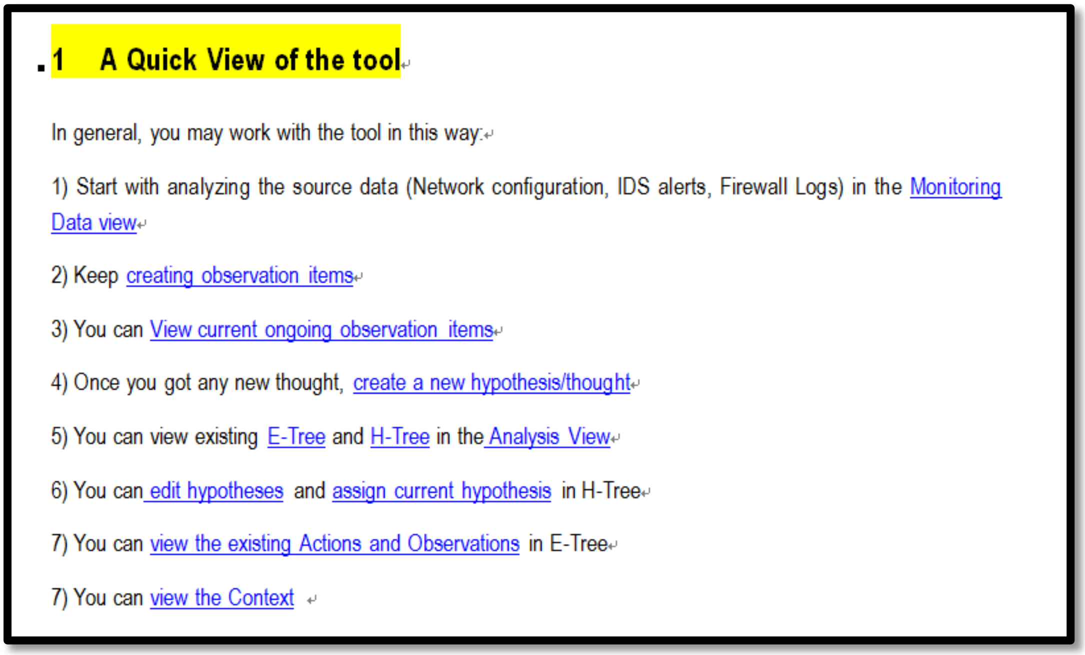
Figure 7. Pages 3-4 of the post-task questionnaire.

Tasks and Stimuli

The task of the subject is to analyze data sources (e.g., network topology and policy, IDS alerts, firewall logs), which can be presented in tabular forms or through visualization displays, about the computer network of a large organization to identify suspected attacks, type of attacks, key events and evidence, and associated hypotheses/questions to guide further investigation or to draw a conclusion.

Training of the Analytical Reasoning Support Tool called ARSCA

Before performing the task, the subject watches a training video to learn to use ARSCA for filtering network data (e.g., IDS alert, firewall log), selecting data entries (i.e., observations), and writing down his/her thoughts (i.e., hypotheses) associated with the data entries using the tool. A set of self-evaluation questions is provided to the subject at the end of the training. A summary of the functions and features of ARSCA is also provided in a handbook, which is made available to the subjects so that they can refer to it for any questions they may have about the tool while performing the task. Figure 8 is the list of key functions of ARSCA that are summarized in the ARSCA Handbook, as well as in the Task Description document, which the subject reads before performing the task.



1 A Quick View of the tool

In general, you may work with the tool in this way:

1) Start with analyzing the source data (Network configuration, IDS alerts, Firewall Logs) in the Monitoring Data view

2) Keep creating observation items

3) You can View current ongoing observation items

4) Once you got any new thought, create a new hypothesis/thought

5) You can view existing E-Tree and H-Tree in the Analysis View

6) You can edit hypotheses and assign current hypothesis in H-Tree

7) You can view the existing Actions and Observations in E-Tree

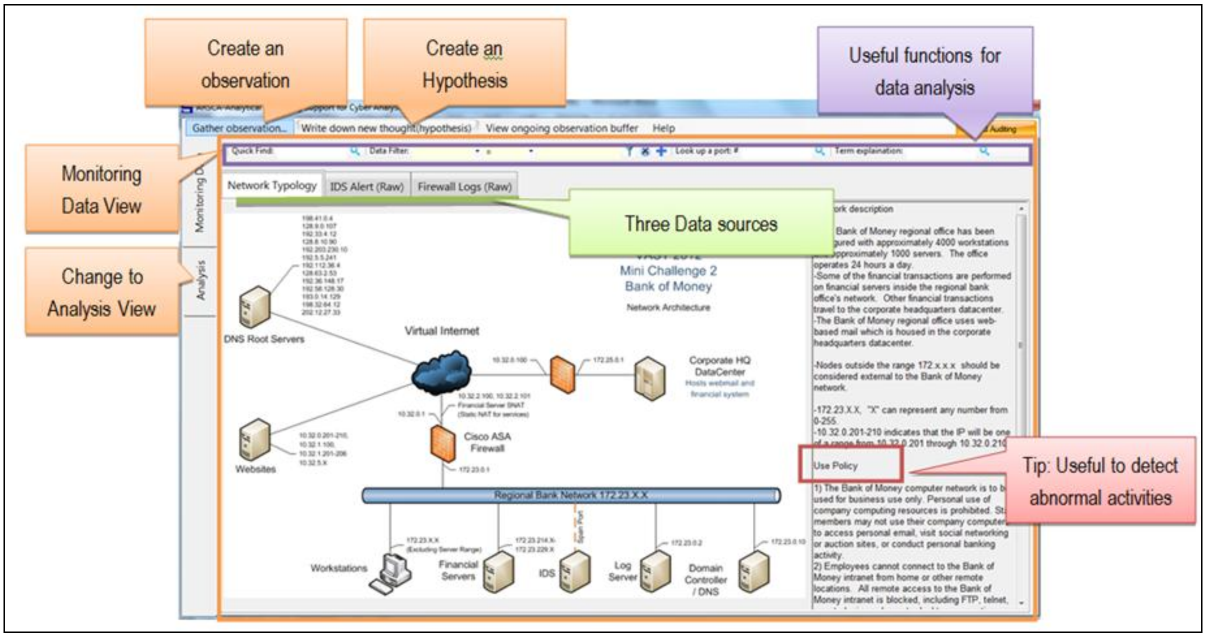
7) You can view the Context

Figure 8. A Summary of Key Functions of ARSCA.

Performing the Task of Network Analysis

After completing the training, the subject proceeds to conduct an intrusion detection task using ARSCA, which provides two views to the subject: (1) a data monitoring view, and (2) an analysis view. Figure 9 is an exemplar screenshot of ARSCA, which is shown with tabs on the left corresponding to the two views. The figure shows an exemplar ARSCA screen in the data view. Also, the screenshot shows the top-level tabs for creating an observation and for creating an associated hypothesis. It also highlights the functions that are useful for browsing, searching, and filtering network security data. Figure 10 shows an example of the data monitoring view, in which the subject can select observations of interests using the space bar or taking a screen shot. The subject can also double-click on any field (e.g., Destination IP) to copy it to the clipboard, and later paste it into the Data Filter or the “Quick Find” field on top of the view.

Figure 11 gives an example of the analysis view, which displays the current E-tree and the current H-tree constructed by an analyst. The analyst can select a node in either tree to view detailed information about them. For example, figure 7 shows the detailed information about a hypothesis (including its current truth value and description) selected by the analyst from the H-tree.



Create an observation

Create an Hypothesis

Useful functions for data analysis

Monitoring Data View

Change to Analysis View

Three Data sources

Tip: Useful to detect abnormal activities

ork description

Bank of Money regional office has been gured with approximately 4000 workstations pproximately 1000 servers. The office operates 24 hours a day.
-Some of the financial transactions are performed on financial servers inside the regional bank office's network. Other financial transactions travel to the corporate headquarters datacenter.
-The Bank of Money regional office uses web-based mail which is housed in the corporate headquarters datacenter.

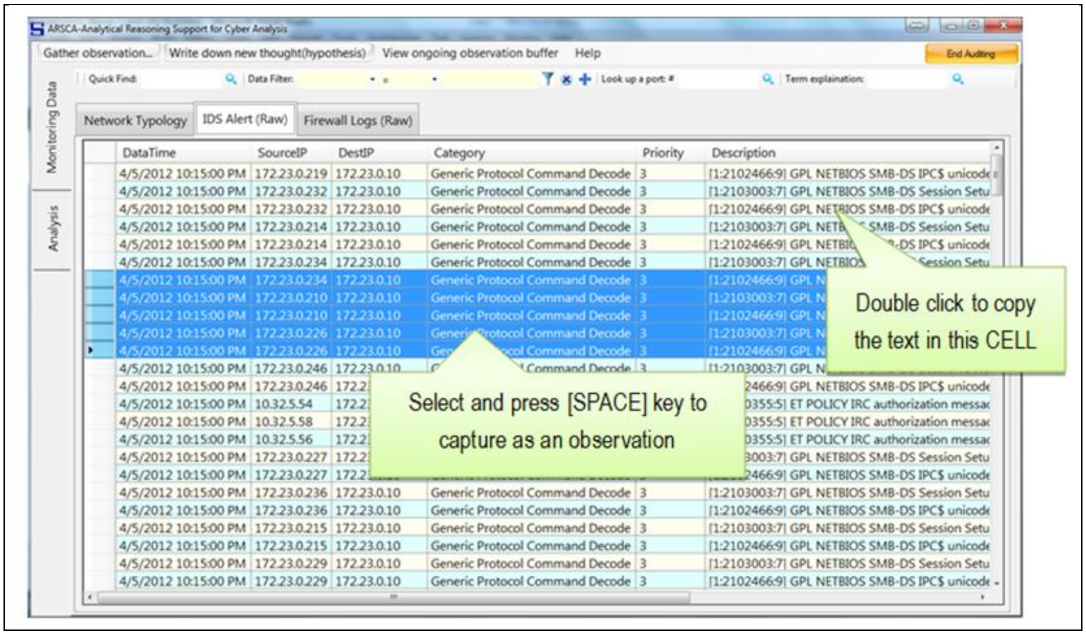
-Nodes outside the range 172.x.x.x should be considered external to the Bank of Money network.

-172.23.X.X, "X" can represent any number from 0-255.
-10.32.0.201-210 indicates that the IP will be one of a range from 10.32.0.201 through 10.32.0.210

Use Policy

1) The Bank of Money computer network is to b used for business use only. Personal use of company computing resources is prohibited. St members may not use their company compute to access personal email, visit social networking or auction sites, or conduct personal banking activity.
2) Employees cannot connect to the Bank of Money intranet from home or other remote locations. All remote access to the Bank of Money intranet is blocked, including FTP, telnet,

Figure 9. Overview of Analytical Reasoning Support Tool for Cyber Analysis (ARSCA).

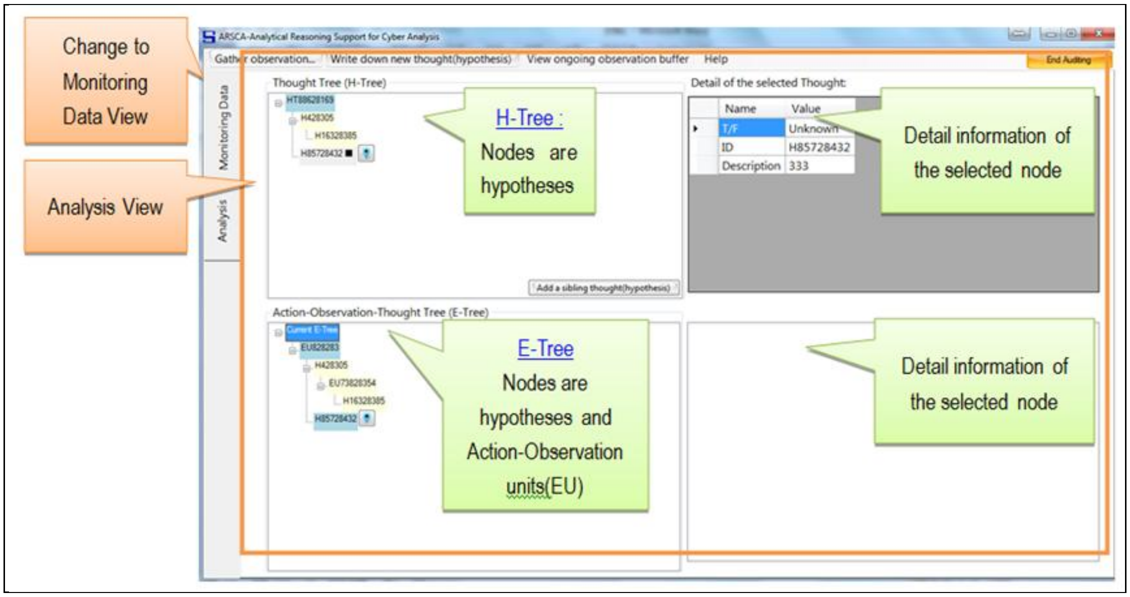


DataTime	SourceIP	DestIP	Category	Priority	Description
4/5/2012 10:15:00 PM	172.23.0.219	172.23.0.10	Generic Protocol Command Decode	3	[1:2102466:9] GPL NETBIOS SMB-DS IPC$ unicode
4/5/2012 10:15:00 PM	172.23.0.232	172.23.0.10	Generic Protocol Command Decode	3	[1:2103003:7] GPL NETBIOS SMB-DS Session Setu
4/5/2012 10:15:00 PM	172.23.0.232	172.23.0.10	Generic Protocol Command Decode	3	[1:2102466:9] GPL NETBIOS SMB-DS IPC$ unicode
4/5/2012 10:15:00 PM	172.23.0.214	172.23.0.10	Generic Protocol Command Decode	3	[1:2103003:7] GPL NETB SMB-DS Session Setu
4/5/2012 10:15:00 PM	172.23.0.214	172.23.0.10	Generic Protocol Command Decode	3	[1:2102466:9] GPL NETBI -DS IPC$ unicode
4/5/2012 10:15:00 PM	172.23.0.234	172.23.0.10	Generic Protocol Command Decode	3	[1:2103003:7] GPL NETBIOS Session Setu
4/5/2012 10:15:00 PM	172.23.0.234	172.23.0.10	Generic Protocol Command Decode	3	[1:2102466:9] GPL N
4/5/2012 10:15:00 PM	172.23.0.210	172.23.0.10	Generic Protocol Command Decode	3	[1:2103003:7] GPL N
4/5/2012 10:15:00 PM	172.23.0.210	172.23.0.10	Generic Protocol Command Decode	3	[1:2102466:9] GPL N
4/5/2012 10:15:00 PM	172.23.0.226	172.23.0.10	Generi Protocol Command Decode	3	[1:2103003:7] GPL N
4/5/2012 10:15:00 PM	172.23.0.226	172.23.0.10	Gen col Command Decode	3	[1:2102466:9] GPL N
4/5/2012 10:15:00 PM	172.23.0.246	172.23.0.10	C Command Decode	3	[1:2103003:7] GPL N
4/5/2012 10:15:00 PM	172.23.0.246	172.2			2466:9] GPL NETBIOS SMB-DS IPC$ unicode
4/5/2012 10:15:00 PM	10.32.5.54	172.2			0355:5] ET POLICY IRC authorization messa
4/5/2012 10:15:00 PM	10.32.5.58	172.2			0355:5] ET POLICY IRC authorization messa
4/5/2012 10:15:00 PM	10.32.5.56	172.2			0355:5] ET POLICY IRC authorization messa
4/5/2012 10:15:00 PM	172.23.0.227	172.2			3003:7] GPL NETBIOS SMB-DS Session Setu
4/5/2012 10:15:00 PM	172.23.0.227	172.2			2466:9] GPL NETBIOS SMB-DS IPC$ unicode
4/5/2012 10:15:00 PM	172.23.0.236	172.23.0.10	Generic Protocol Command Decode	3	[1:2103003:7] GPL NETBIOS SMB-DS Session Setu
4/5/2012 10:15:00 PM	172.23.0.236	172.23.0.10	Generic Protocol Command Decode	3	[1:2102466:9] GPL NETBIOS SMB-DS IPC$ unicode
4/5/2012 10:15:00 PM	172.23.0.215	172.23.0.10	Generic Protocol Command Decode	3	[1:2103003:7] GPL NETBIOS SMB-DS Session Setu
4/5/2012 10:15:00 PM	172.23.0.215	172.23.0.10	Generic Protocol Command Decode	3	[1:2102466:9] GPL NETBIOS SMB-DS IPC$ unicode
4/5/2012 10:15:00 PM	172.23.0.229	172.23.0.10	Generic Protocol Command Decode	3	[1:2103003:7] GPL NETBIOS SMB-DS Session Setu
4/5/2012 10:15:00 PM	172.23.0.229	172.23.0.10	Generic Protocol Command Decode	3	[1:2102466:9] GPL NETBIOS SMB-DS IPC$ unicode

Double click to copy the text in this CELL

Select and press [SPACE] key to capture as an observation

Figure 10. Selecting Observations in the Data Monitoring View of ARSCA.


Change to Monitoring Data View
Analysis View
ARSCA-Analytical Reasoning Support for Cyber Analysis
Gath r observation...
Write down new thought(hypothesis)
View ongoing observation buffer
Help
End Auditing
Monitoring Data
Analysis
Thought Tree (H-Tree)
HT88628169
H428305
H16328385
H85728432
H-Tree :
Nodes are hypotheses
Add a sibling thought(hypothesis)
Detail of the selected Thought:
Detail information of the selected node
Action-Observation-Thought Tree (E-Tree)
Current E-Tree
EU828283
H428305
EU73828354
H16328385
H85728432
E-Tree
Nodes are hypotheses and Action-Observation units(EU)
Detail information of the selected node

Name	Value
T/F	Unknown
ID	H85728432
Description	333

Figure 11. Browsing Hypotheses in the Analysis View of ARSCA.

5. Subjects

The age of subjects is between 18 and 50. The inclusion criterion is that the subject performs cyber security analysis on a daily basis as a part of his/her job function.

Sample Size Justification

The number of subjects is between 12 and 20 so that the time for the subjects to participate in the study does not interfere with their job functions as network analysts at U.S. Army Research Laboratory (ARL). A similar number of subjects have also been used in a previous study about network analysts (*9*).

Compensation

Subjects of the study recruited from ARL do not receive compensation.

Subject Recruitment

Subjects were recruited by Dr. John Yen during his visit to ARL in the summer of 2013. Dr. Yen first described the goal, the A-O-H model, and the tool of the research study to researchers and managers of Network Science Division in Computational and Information Sciences Directorate (CISD). After obtaining their approval, subjects were recruited from network analysts of Network Science Division through their managers. A total of 12 subjects (with different levels of experience) were recruited from Network Science Division of CISD. Additional subjects, if needed, will be recruited by Dr. Robert Erbacher.

6. Procedure

The procedure of the study includes five major steps: (1) Subjects arrive at the research site, are met, given an overview of the study, and allowed to read the consent form. After obtaining informed consent, each subject will then be assigned a randomly generated anonymous identification number to protect his/her personal information and identity. This step takes an average of 5 min. (2) Subjects fill out the Pre-Task Questionnaire. The average time of this step is 10 min. (3) Subjects receive self-guided training by watching training video and following self-assessment at the end of training. On average, this step takes 20 min for the first scenario. This step is estimated to take 5 min for subsequent scenarios. (4) Subjects perform the task described in the previous section. This step takes an average of 60 min. (5) Subjects fill out the Post-Task Questionnaire. The average time for this step is 25 min. The entire procedure takes, on the average, 2 hfor the first session. The expected time for subsequent sessions is 100 min for each session. There is no audio recording or video recording during any part of the procedure. Furthermore, researchers do not interact with the subjects from step 2 to step 5.

Research data (e.g., Pre-Task Questionnaire, Post-Task Questionnaire, and traces of A-O-H analytical reasoning process of subjects) generated from the study will be reviewed by ARL for OPSEC compliance before they are released to the investigators.

Training

The training component of the procedure includes three sub-steps. First, the subject reads "Basic Information," which describes background information of the task, including the network topology of the enterprise network, the IP addresses involved in the network, and the data to be used in the task (e.g., IDS alerts, Firewall logs). Second, the subject learns about A-O-H model and the Analytical Reasoning Support for Cyber Analysis (ARSCA) tool by watching training videos and by reading corresponding sections in the ARSCA Handbook. The last step of training is for the subject to conduct a self-assessment about key functions of the ARSCA tool.

Pilot Study or Pilot Testing

A pilot study has been conducted both at The Pennsylvania State University and at ARL's Adelphi Laboratory Center (ALC). The subjects of the pilot study at ALC were network analysts recruited from ALC. The results of the pilot provided important feedback that improves the data filtering function of the tool, the user friendliness of the interface, and the training material of the study. The pilot study confirmed that the scenario of the task is realistic and is at a suitable level of difficulty. The pilot study also confirmed that the time required for completing the task is, on the average, an hour, and the total time required for completing one session (including pre-task questionnaire, training, performing the task, and post-task questionnaire) is, on the average, 2 h.

7. Experimental Design

This is an observation-centric study. Therefore, there is no control group. In the previous sections, we describe the research objectives, the equipment, the recruiting of subjects, the procedure, the training, the Pre-Task Questionnaire, the task, and the Post-Task Questionnaire for the experiment. The primary research hypothesis of the study is that the A-O-H model can capture the analytical reasoning process of the cyber security analysts. The secondary research hypothesis is that the A-O-H model can capture the differences of the analytical reasoning process between experts and less-experienced analysts. The Pre-Task Questionnaire is designed to collect information related to the experience level of analysts so that we can compare the analytical processes of experts with those of less-experienced analysts. For this reason, subjects were recruited from analysts with different level of experiences. The scenarios of the sessions were designed by extracting four 10-min intervals from the entire data set of VAST Challenge. Because the four scenarios are part of one multi-step cyber attack, there are logical relationships between the scenarios. Because the four sessions are designed to be independent tasks for the analysts, we arrange the four scenarios for the experiment into the following order to weaken the potential logical relationship between one session and the next one in the experiment: subjects starts with scenario 2, followed by scenario 4, followed by scenario 1, and followed by scenario 3.

The results of this experiment will include one or more papers that describe the findings in validating the A-O-H model, and one or more papers that identify and compare differences of the analytical reasoning process between experts and less-experienced analysts. These results can contribute to the design of improved training of network analysts, especially those involved in CNDSP. For instance, the differences between expert analysts and less-experienced analysts can be used to develop training objectives, training models, and an intelligent personalized training tool that tailors the training objectives to individual analysts based on the result of assessing their analytical reasoning process before, during, and after training.

The results of this study can also contribute to improving training for Soldiers to increase their awareness and understanding about cyber security.

Finally, the findings of this study can contribute to the design of STEM education materials for K-12 students to increase their interests and awareness for cyber security-related studies and careers, and STEM-related education and professional opportunities in general.

8. Data Analysis

The data collected will be analyzed using a combination of qualitative methods and quantitative methods. Both the accuracy of the analysts' results and the time of completing the task (for each scenario) will be analyzed. For example, the analytical reasoning traces and the experience trees collected from subjects will be analyzed in multiple ways. First, we will identify the ground truths in the experience trees. Second, we will investigate whether the ground truth identified in the E-trees form a tight logical relationship. Third, we will invite a domain expert panel to evaluate the trees to see whether the tree does a good job in capturing the analytical reasoning process. Finally, we will investigate the use of machine learning methods together with cognitive task analysis for analyzing the traces to identify differences between experts and less-experienced subjects (*10, 11*).

8.1 Risks and Discomforts and Mitigation of Each Risk and Discomfort

Risk: A loss or breach of confidentiality may be a potential risk. Mitigation: Each subject is assigned a randomly generated anonymous identification number. The informed consent form is stored and secured in a password protected file in room 301F, Information Sciences and Technology Building, The Pennsylvania State University (University Park) in a password-protected file.

There are no additional risks for subjects to participate in this research beyond those experienced in everyday life of a typical cyber security analyst. None of the questions in the questionnaires used in the study are about personal identifiable information.

8.2 Benefits

The subject can benefit from the pre-experiment "cyber security analyst" training (designed by the researchers) as a useful learning experience. Furthermore, their participation in the study, especially the reflection they perform about the intrusion detection task after they perform the task, may provide new insights about their analytical reasoning process. Finally, their contributions and results of the study can improve the scientific knowledge and understanding about cognitive processes of cyber analysts, which can contribute to improving the quality of on-job training, training new analysts, and supporting their daily network analysis task more effectively in the near future.

8.3 Confidentiality or Anonymity

The data collected from this study, after review by ARL for OPSEC compliance, will be stored and secured at 301F IST building in a password-protected file. Penn State's Office for Research Protections, the Institutional Review Board, and the Office for Human Research Protections in the Department of Health and Human Services may review records related to this research study.

Representatives of the U.S. Army Medical Research and Material Command (USAMRMC) are eligible to review all research related records. In the event of a publication or presentation resulting from the research, no personally identifiable information will be shared. There will be neither video nor audio recording during any portion of the study. No photographs will be taken during the study, either.

The participants' personal information remains confidential. The study requires obtaining basic information from participants, and no personal information besides a name and signature for the consent form is required. This study uses the participants' responses, performance, and demographic information related to the study in the publication of the research. However, we provide a randomly generated anonymous identification number to protect their identity for data analysis and for reporting results in publications.

9. References

1. Feigenbaum, E. Knowledge Engineering: The Applied Side of Artificial Intelligence. in *Proc. of a Symposium on Computer Culture: the Scientific, Intellectual, and Social Impact of the Computer*, New York, NY, pp. 91–107, 1984.

1. Giacobe, N. A. Data Fusion in Cyber Security: First Order Entity Extraction from Common Cyber Data. In *Proc. of SPIE* Vol (Vol. 8408), 2012.

2. Morin, B.; Mé, L.; Debar, H.; Ducassé, M. A Logic-Based Model to Support Alert Correlation in Intrusion Detection. *Information Fusion* **2009**, *10* (4), 285–299.

3. Tabia, K.; Benferhat, S.; Leray, P.; Mé, L. Alert Correlation in Intrusion Detection: Combining AI-Based Approaches for Exploiting Security Operators‟ Knowledge and preferences. In *The 3rd IJCAI-11 Workshop on Intelligent Security (SECART-11)*, (pp. 42–49), 2011.

4. Ou, X.; Boyer, W. F.; McQueen, M. A. A Scalable Approach to Attack Graph Generation. In *Proc. of the 13th ACM CCS* (pp. 336–345), 2006.

5. Chen, P. C.; Liu, P.; Yen, J.; Mullen, T. Experience-Based Cyber Situation Recognition Using Relaxable Logic Patterns. In *CogSIMA, IEEE International Multi- Disciplinary Conference* (pp. 243–250), 2012.

6. Yen, J.; McNeese, M.; Mullen, T.; Hall, D.; Fan, X.; Liu, P. RPD-Based Hypothesis Reasoning for Cyber Situation Awareness. *Cyber Situational Awareness* **2010**, 39–49.

7. Pirolli, P.; Card, S. The Sensemaking Process and Leverage Points for Analyst Technology as Identified Through Cognitive Task Analysis. In *Proc. of International Conference on Intelligence Analysis*, 2005.

8. Zhong, C.; Kirubakaran, D. S.; Yen, J.; Liu, P.; Hutchinson, S.; Cam, H. How to Use Experience in Cyber Analysis: An Analytical Reasoning Support System. in *Proceedings of IEEE Conference on Intelligence and Security Informatics (ISI)*, 2013.

9. Giacobe, N. A. Measuring the Effectiveness of Visual Analytics and Data Fusion Techniques on Situation Awareness in Cybersecurity, Ph.D. thesis, Information Sciences and Technology, The Pennsylvania State University, 2012.

10. D’Amico, A.; Whitley, K.; Tesone, D.; O’Brien, B.; Roth, E. Achieving Cyber Defense Situational Awareness: A Cognitive Task Analysis of Information Assurance Analysts. in *Proc. of 49th Annual Meeting of Human Factors and Ergonomics Society*, pp. 229–233, 2005.

11. Erbacher, R.; Frincke, D. A.; Wong, P. C.; Moody, S.; Fink, G. A Multi-Phase Network Situational Awareness Cognitive Task Analysis. *Information Visualization* **2010**, *9* (3), 204–219.

12. Hall, D. L.; Llinas, J. An Introduction to Multi-Sensor Data Fusion. *Proceedings of the IEEE* **1997**, *85* (1), 6–23.

13. Endsley, M. R. Toward a Theory of Situation Awareness in Dynamic Systems. *Human Factors* **1995**, *37* (1), 32–64.

NO. OF COPIES	ORGANIZATION
1 (PDF)	DEFENSE TECHNICAL INFORMATION CTR DTIC OCA
2 (PDFS)	DIRECTOR US ARMY RESEARCH LAB RDRL CIO LL IMAL HRA MAIL & RECORDS MGMT
1 (PDF)	GOVT PRINTG OFC A MALHOTRA
2 (PDFS)	COLLEGE OF INFORMATION SCIENCES AND TECHNOLOGY THE PENNSYLVANIA STATE UNIVERSITY PENG LIU JOHN YEN
3 (PDFS)	DIRECTOR US ARMY RESEARCH LAB RDRL CIN D ROBERT ERBACHER WILLIAM GLODEK RENEE E. ETOTY